

Ifw

<b>TRANSMITTAL OF INFORMATION DISCLOSURE STATEMENT</b> Under 37 CFR 1.97(b), (c), or (d)			Docket No. <b>SRI/3928-9</b>	
In re Application of: <b>Porras, et al.</b>				
Serial No. <b>10/805,729</b>	APR 04 2006	Filing Date <b>03/22/2004</b>	Examiner <b>Ayaz R. Sheikh</b>	Group Art Unit <b>2131</b>
Title: <b>NETWORK SURVEILLANCE</b>				

Address to:  
Assistant Commissioner for Patents  
Washington, D.C. 20231

### 37 CFR 1.97(b)

1. ☒ The Information Disclosure Statement submitted herewith is being filed within three months of the filing of a national application other than a continued prosecution application under 37 CFR 1.53(d); within three months of the date of entry of the national stage as set forth in 37 CFR 1.491 in an international application; before the mailing of a first Office Action on the merits; or before the mailing of a first Office Action after the filing of a request for continued examination under 37 CFR 1.114.

### 37 CFR 1.97(c)

2. ☐ The Information Disclosure Statement submitted herewith is being filed after the period specified in 37 CFR 1.97(b), but prior to the mailing date of a Final Action under 37 CFR 1.113, a Notice of Allowance under 37 CFR 1.311, or an Action that otherwise closes prosecution in the application, and is accompanied by the statement or fee as indicated below.

### 37 CFR 1.97(d)

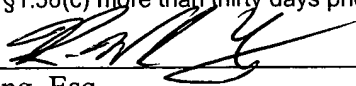
3. ☐ The Information Disclosure Statement submitted herewith is being filed after the period specified in 37 CFR 1.97(c), but on or before payment of the issue fee and is accompanied by the statement and fee as indicated below.

### Required Statements and/or Fees Under 37 CFR 1.97(c) or (d)

- ☐ Each item of information contained in the accompanying Information Disclosure Statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the Information Disclosure Statement. (37 CFR 1.97(e)(1))
- ☐ No item of information in the accompanying Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned person, after making reasonable inquiry, no item of information contained in the accompanying Information Disclosure Statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the Information Disclosure Statement. (37 CFR 1.97(e)(2))
- ☐ The fee set forth in 37 CFR 1.17(p). Please credit any overpayment or charge any insufficiencies to deposit account number 20-0782.

### 37 CFR §1.704(d)

4. ☐ Each item of information in the accompanying Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart application and this communication was not received by any individual designated in 37 CFR §1.56(c) more than thirty days prior to the filing of the Information Disclosure Statement.

  
Kin-Wah Tong, Esq.

Reg. No. 39,400

**Patterson & Sheridan, LLP**

**Attorneys at Law**

**595 Shrewsbury Avenue, Suite 100**

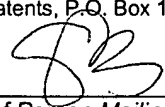
**Shrewsbury, New Jersey 07702**

**732-530-9404**

Dated: 3/31/06

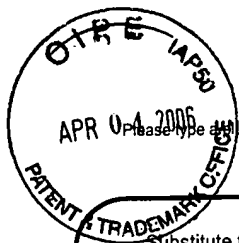
### Certification of Mailing under 37 C.F.R. 1.10

I certify that this document is being deposited on with the U.S. Postal Service in an first class envelope and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

  
Signature of Person Mailing Correspondence

**Sujata Barot**

Typed or Printed Name of Person Mailing Correspondence



APR 04 2006

Please type plus sign (+) inside this box →



PTO/SB/08a (08-03)

Approved for use through 07/31/2006. OMB 0651-0031  
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Substitute for form 1449A/PTO

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**

(Use as many sheets as necessary)

Application Number	10/805,729
Filing Date	03/22/2004
First Named Inventor	Porras et al.
Group Art Unit	2131
Examiner Name	Ayaz R. Sheikh
Attorney Docket Number	SRI/3928-9
Submission Date	March 31, 2006

Sheet 1

of 3

**U.S. PATENT DOCUMENTS**

Examiner Initials*	Cite No. <sup>1</sup>	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code <sup>2</sup> (if known)			
	A1	6,067,582	05-2000	Smith, et al.	
	A2	6,119,236 A	09-2000	Shipley, P.M.	
	A3	6,192,392	02-2001	Ginter	
	A4	6,269,456	07-2001	Hodges et al.	
	A5	6,275,942 B1	08-2001	Bernhard et al.	
	A6	6,298,445	10-2001	Shostack et al.	
	A7	6,324,656	11-2001	Glechauf et al.	
	A8	2002/0019870	02-2002	Chirashnya et al.	
	A9	6,405,318	06-2002	Rowland, C. H.	
	A10	6,442,694 B1	08-2002	Bergman et al.	
	A11	6,477,651 B1	11-2002	Teal, D.M.	
	A12	6,529,954 B1	03-2003	Cookmeyer et al.	
	A13	6,535,227	03-2003	Fox et al.	
	A14	6,532,543	03-2003	Smith et al.	
	A15	6,546,493 B1	04-2003	Magdych et al.	
	A16	2003/0145226	07/31/2003	Bruton III et al	
	A17	2003/0172166	09/11/2003	Judge et al.	
	A18	6,553,378 B1	04-2003	Eschelbeck, G.	

**FOREIGN PATENT DOCUMENTS**

Examiner Initials*	Cite No. <sup>1</sup>	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T <sup>6</sup>
		Country Code <sup>3</sup> -Number <sup>4</sup> -Kind Code <sup>5</sup> (if known)				
	B1	WO 03/077071	09/18/2003	Giphertrust, Inc.		
	B2	WO 02/101516 A2	12/19/2002	Intruvert Networks		
	B3	WO 99/57625	11/11/1999	PRC Inc.		
	B4					
	B5					

Examiner

Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. <sup>1</sup> Applicant's unique citation designation number (optional). <sup>2</sup> See Kinds Codes of USPTO Patent Documents at [www.uspto.gov](http://www.uspto.gov) or MPEP 901.04. <sup>3</sup> Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>4</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>5</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. <sup>6</sup> Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450. If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.





Substitute for form 1449B/PTO

# **INFORMATION DISCLOSURE STATEMENT BY APPLICANT**

(Use as many sheets as necessary)

Sheet 3

3

Application Number	10/805,729
Filing Date	03/22/2004
First Named Inventor	PORRAS et al.
Group Art Unit	2131
Examiner Name	Ayaz R. Sheikh
Attorney Docket Number	SRI/3928-9
Submission Date	March 31, 2006

## **NON PATENT LITERATURE DOCUMENTS**

Examiner Initials*	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T <sup>2</sup>
	C1	SHOSTACK, A., "An overview of SHTTP, pp 1-7, May 1995.	
	C2	RADLAN, "Intrusion Detection, Extend the Monitoring and Protection of Your Network", Radlan White Paper, pp. 1-7, February 1999	
	C3	ALMGREN, et al., "A lightweight Tool for Detecting Web Server Attacks," Network and Distributed Systems Security ( NDSS 2000) Symposium Proceedings, pp. 157-170, 2000. Copy provided is marked as pp.1-14	
	C4	ALMGREN, et al., "Application-Integrated Data Collection for Security Monitoring, " From Recent Advances in Intrusion Detection (RAID 2001) Springer, Davis, California, pp. 22-36 October 2001(copy comprises of pp. 1-21)	
	C5	DANIELS, et al. " A network Audit System for Host-based Intrusion Detection (NASHID) in Linux," 16 <sup>th</sup> annual Computer Security Application Conference (ACSAC 00) pp. 1-10, December 2000.	
	C6	DANIELS, et al. "Identification of Host Audit Data to Detect Attacks on Low-Level IP Vulnerabilities, "J. Computer Security, 7 (1), pp. 3-35, 1999.	
	C7	DAYIOGLU, "APACHE Intrusion Detection Module," <a href="http://yunus.hacettepe.edu.tr/~burak/mod_id">http://yunus.hacettepe.edu.tr/~burak/mod_id</a> , pp.1-6, date Unknown, Downloaded 11/10/2003.	
	C8	HOLLANDER, Y., "The Future of Web Server Security: Why your web site is still vulnerable to attack," <a href="http://www.cgisecurity.com/lib/wpfuture.pdf">http://www.cgisecurity.com/lib/wpfuture.pdf</a> , pp. 1-9, allegedly posted 2000.	
	C9	LINDQVIST, et al, "eXpert-BSM: A host-based Intrusion Detection Solution for Sun Solaris," Proc 17 <sup>th</sup> Annual Computer security Application Conference, pg 240-251, December 2001.(copy provided comprises of pp. 1-12)	
	C10		
	C11		
	C12		

Examiner

Date Considered

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450. If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.



Docket No.: SRI/3928-9  
Applicant: PORRAS, et al.  
Filed: 3/22/04  
Serial Number 10/805,729

The following has been received in the U.S. Patent and Trademark Office on the date stamped hereupon:

☒ Information Disclosure Statement  
☐ Information Disclosure Statement with Deposit Account Transaction  
☐ ( ) Abstracts or Translations  
☒ ( 3 ) Foreign Patent Documents  
☒ ( 9 ) Non-Patent Literature Documents  
☐ Transmittal Letter (2 copies)  
☐ Fee Transmittal (2 copies) Other \_\_\_\_\_  
☒ Form 1449  
\_\_\_\_\_ Mail Certificate, dated \_\_\_\_\_  
Log # \_\_\_\_\_